Contents

State Library of New South Wales cataloguing-in publication data

New South Wales. Audit Office.

Guide to better practice : e-ready, e-steady, e-government : e-government readiness assessment guide for government agencies / [The Audit Office of New South Wales]

0734721250

1. Internet in public administration - New South Wales. 2. Administrative agencies - New South Wales - Data processing. I. Title: e-ready, e-steady, e-government.

352.3809944

September 2001

Implementing E-government - being ready

The NSW Government, like many other governments world wide, has recognised that the transformation from traditional government to electronic government is one of the most important public policy issues of our time.

It is also recognised that e-government is not simply about implementing a new IT system. It is about changing business models and processes to do things differently and better.

Information technology offers the solutions, but e-government is about changing the way the agency operates. The Audit Office agrees that it is an issue which all senior management needs to be across.

The purpose of this document is to assist agencies in meeting the challenges of exploiting the benefits and managing the risks which e-government presents. Being 'e-ready' and managing the transition to e-government will not happen by chance. It is difficult and requires a careful and concerted effort.

This guide draws from the research assembled in the performance audit, e-government - Use of the Internet and related technologies to improve public sector performance (September 2001). It addresses issues at the agency level, in a self-help guide format.

The guide is not a comprehensive plan for implementing e-government in an agency. Neither is it a series of compliance or reporting requirements. Rather, it is designed to provide a simple assessment tool to assist in focusing high-level awareness across the range of issues required for the efficient and effective implementation of e-government. To avoid duplicating others' work, this guide draws upon selected guidance material produced elsewhere, and references those in 'help' sections included under each element examined.

Agencies also need to be aware of the raft of policies, memoranda and guidelines published by NSW central government agencies to assist agencies in managing e-government implementation. Information currently available is referenced in this guide.

The guide should not be relied upon as legal advice. Agencies need to make their own arrangements for such advice.

The guide, the sector-wide performance audit report and other information on our e-government auditing work are all available via our web-site at www.audit.nsw.gov.au.

The Audit Office is happy to receive feedback on this guide and should it be necessary the electronic version will be updated on our web-site to reflect circumstances and experiences.

Leadership and Governance

SUCCESSFUL E-GOVERNMENT IMPLEMENTATION REQUIRES STRONG LEADERSHIP, EFFECTIVE PLANNING, A FOCUS ON RESULTS, AND ONGOING MONITORING

BETTER PRACTICE PRINCIPLES

- Senior management understands the opportunities and risks offered by e-government, and clearly demonstrates commitment to implementing it for the benefit of citizens
- Agency planning addresses e-government and provides a road map for the future, consistent with the Government's e-government reform directions
- Priorities are determined, targets established, incentives provided, results measured and personnel held accountable for meeting goals
- Processes are redesigned to take advantage of the full potential of technology
- Working cooperatively with other agencies to advance e-government is encouraged
- Better e practices are monitored and adopted

RISKS TO BE MANAGED

- Inaction or misdirected efforts
- Insufficient reason to pursue more fundamental reform
- Business processes not redesigned to make full use of the new technologies
- Services put on-line are the easiest not the best
- E-government progress inconsistent across the agency
- Government-wide directions not followed
- Duplication of effort
- Projects fail to deliver on time and budget
- Inability to link and share information with potential partners
- Maintaining inefficient paper-based transactions longer than necessary
- Inability to measure and assess achievements

HELP

- ANAO, Internet delivery decisions - A Government Program Manager's Guide, components 1, 2 and 5
- NSW Office of Information Technology: memoranda; guidelines; case studies (various)
- Information Management and Technology Blueprint for NSW - A well connected future
- connect.nsw, an Internet strategy for NSW and connect.nsw implementation framework
- NSW Treasury, Risk Management and Internal Control Toolkit
- National Electronic Commerce Coordinating Council (US): E-government strategic planning - A White Paper; Risk assessment guidebook for e-government/e commerce; Critical business issues in the transformation to electronic government
- Office for Government On-line (Cwth), On-line action plan guidelines

Checklist

	Performing	Progressing	Potential
Senior management and staff demonstrate a clear commitment to the implementation of e-government.	☐	☐	☐
A unified direction for e-government is set for the agency, with clear articulation of objectives.	☐	☐	☐
E-government is an integral part of the agency's corporate, strategic and business planning.	☐	☐	☐
Opportunities for working with other organisations are explored continually.	☐	☐	☐
Measurable targets/results and milestones for e-government are documented in agency planning.	☐	☐	☐
E-government activities and progress are monitored against plans.	☐	☐	☐
Initiatives promising significant performance improvements are given priority, particularly those offering the potential to redesign processes.	☐	☐	☐
Better e-government practices are identified and applied.	☐	☐	☐
Personnel are held accountable for achieving the agency's e-government goals.	☐	☐	☐
A steering committee (or similar) has been established for the oversight, development and maintenance of e-government.	☐	☐	☐
A chief information officer (CIO) is nominated and carries out activities in accordance with government guidelines.	☐	☐	☐
The steering committee or CIO controls technology acquisition and sets binding standards.	☐	☐	☐
The person or committee responsible for monitoring results has sufficient authority and resources to identify issues and initiate corrective action.	☐	☐	☐
Central government directions, policies, guidelines and procedures are followed in developing e-government initiatives.	☐	☐	☐
E-government risks are identified, planned for and managed.	☐	☐	☐
E-government project management is comprehensive, rigorous and systematic.	☐	☐	☐
Branches/divisions:			
◖ communicate effectively with each other about e-government	☐	☐	☐
◖ work together well to advance e-government.	☐	☐	☐
A staged approach to implementation is adopted.	☐	☐	☐

THE BENEFITS OF E-GOVERNMENT CAN BE PROFOUND, BUT SUBSTANTIAL UP-FRONT FINANCIAL INVESTMENT MAY BE REQUIRED

Funding

BETTER PRACTICE PRINCIPLES

- A long-term view of the return on investment is taken - a recognition of the need to invest up-front to generate longer term changes
- The costs of initial development and continued operation of e-government are estimated, funded and monitored
- Projects which will deliver best value for money and significant change are funded
- Innovative funding arrangements are explored and adopted where appropriate
- Opportunities for joint projects and funding are pursued

RISKS TO BE MANAGED

- E-government funding decisions based on unsound business cases
- Thinly spread funding leading to system patching and piecemeal solutions
- Inadequate funding to develop and maintain initiatives which offer best value for money
- Options for innovative funding not pursued
- Valuable resources wasted in preparing unsuccessful funding submissions
- Return on e-government investment not well measured and monitored

HELP

- ANAO, Internet delivery decisions - A Government Program Manager's Guide, components 2, 4 and 5
- NSW Office of Information Technology: memoranda, guidelines, case studies (various)
- NSW Premier's Department, Business Case Guidelines
- NSW Treasury, Circulars
- National Electronic Commerce Coordinating Council (US): E-government strategic planning - A White Paper; Risk assessment guidebook for e-government/e commerce; Critical business issues in the transformation to electronic government

Checklist

	Performing	Progressing	Potential
The agency has a strategy for funding e-government projects.	☐	☐	☐
The agency's funding approaches:			
◖ are flexible and able to respond to the rapid pace of technological change	☐	☐	☐
◖ recognise that costs are likely to be higher and benefits lower in initial years.	☐	☐	☐
Funding is prioritised to projects promising significant performance improvement and best value for money.	☐	☐	☐
Funding levels are consistent with:			
◖ citizen expectations	☐	☐	☐
◖ the objectives for e-government.	☐	☐	☐
Funding is adequate for:			
◖ initial development	☐	☐	☐
◖ ongoing maintenance and operations.	☐	☐	☐
Joint funding opportunities with other agencies are explored.	☐	☐	☐
Options for innovative or alternative funding approaches made possible by e-government are pursued.	☐	☐	☐
Central agency guidelines (including business case and benefit realisation guidelines) are followed.	☐	☐	☐
There is close liaison with central agency officers responsible for assessing e-government funding submissions.	☐	☐	☐
Systems are in place to monitor and account for expenditures.	☐	☐	☐
Return on investment is measured in a consistent way.	☐	☐	☐

People

THE COMPETENCY AND COMMITMENT OF THE INDIVIDUALS DEVELOPING, IMPLEMENTING, AND SUPPORTING E-GOVERNMENT DRIVE THE EFFECTIVENESS AND EFFICIENCY THAT CAN BE ACHIEVED

BETTER PRACTICE PRINCIPLES

- Competencies required for an e-government operating environment are established and defined
- Staffing requirements are regularly evaluated to ensure the agency has a sufficient number of personnel with the right competencies for the e-government operating environment
- Personnel in the agency know their roles and responsibilities in relation to e-government and have sufficient authority to perform them
- The right skills are available, internally, through partnerships, or by contract
- Employment arrangements provide the flexibility to implement and manage changes arising from e-government
- Training is adequate to meet and maintain e-government skills
- Incentives are adequate to attract and retain highly skilled personnel and to promote strong performance
- Competencies include sourcing and buying technology, change management, contract negotiation and management, managing highly skilled information and communications technology (ICT) contractors/consultants, system security, project management, risk management, relationship management, and implementing application enhancements

RISKS TO BE MANAGED

- Lack of commitment to e-government reform
- Personnel not possessing required skills
- Personnel with required skills not available
- Ineffective management of consultants and loss of agency corporate knowledge
- Employment frameworks make change difficult
- Benefits available through technology not fully realised
- Training not preparing personnel well for new work methods
- Inability to retain key personnel

HELP

- National Electronic Commerce Coordinating Council (US): E-government strategic planning - A White Paper; Risk assessment guidebook for e-government/e-commerce; Critical business issues in the transformation to electronic government
- NSW Office of Information Technology: memoranda, guidelines, case studies (various)
- NSW Premier's Department Circulars; Personnel Handbook
- NSW Premier's Memoranda, various from time to time

Checklist

	Performing	Progressing	Potential
Personnel are kept informed about the necessity and benefits of e-government.	☐	☐	☐
Personnel understand the move toward e-government, what their roles will be and expectations of them.	☐	☐	☐
The agency provides incentives that:			
◖ promote acceptance of technology developments and changes to work processes	☐	☐	☐
◖ encourage re-skilling for the new work arrangements	☐	☐	☐
◖ attract and retain qualified, highly skilled personnel	☐	☐	☐
◖ encourage superior performance.	☐	☐	☐
The agency's employment arrangements provide the flexibility to implement and manage changes arising from e-government.	☐	☐	☐
The organisational culture supports a mobile, flexible and adaptable workforce.	☐	☐	☐
Key e-government positions have been identified, defined and filled.	☐	☐	☐
E-government competencies are determined.	☐	☐	☐
Personnel skill sets are assessed continually and compared to those needed for e-government.	☐	☐	☐
Training and support keep personnel skill sets current with e-government developments.	☐	☐	☐
Changes in personnel needs are acted on promptly.	☐	☐	☐
Opportunities for sharing highly skilled personnel between agencies are explored and implemented where appropriate.	☐	☐	☐
Mechanisms are in place to transfer the knowledge gained by consultants/contractors to the agency.	☐	☐	☐

Legal

E-GOVERNMENT INITIATIVES NEED TO COMPLY WITH LEGISLATIVE REQUIREMENTS AND HAVE LEGAL STANDING

BETTER PRACTICE PRINCIPLES

- A legal framework supporting e-government is in place
- Legal developments affecting e-government are monitored and necessary action is taken
- Agency legislation is reviewed to determine and address possible e-government impediments
- E-government business practices comply with statutory requirements
- The legal standing of electronic transactions is assured
- Legal liability is defined and made known to all parties involved in e-government

RISKS TO BE MANAGED

- Legislation entrenches paper-based transactions
- Inability to enforce on-line transactions
- Potential litigation and legal liability
- Lack of progress due to hesitancy about legal issues
- Opportunities for eliminating cumbersome transactions missed

HELP

- ANAO, Internet delivery decisions - A Government Program Manager's Guide, component 7
- National Electronic Commerce Coordinating Council (US): E-government strategic planning - A White Paper; Risk assessment guidebook for e-government/e-commerce; Critical business issues in the transformation to electronic government
- NSW Office of Information Technology: memoranda, guidelines, case studies (various)
- NSW Electronic Transactions Act 2000
- NSW Treasury Circulars
- NSW Treasurer's Directions

Checklist

	Performing	Progressing	Potential
Legal advice is obtained during business analysis, system design and implementation to identify and resolve legal issues or impediments.	☐	☐	☐
Legislation and case law related to e-government activities are monitored to:			
◖ ensure compliance	☐	☐	☐
◖ identify emerging legislative issues/impediments.	☐	☐	☐
Legal standing has been established for electronic contracts/transactions.	☐	☐	☐
Legal advice has approved the methods for ensuring:			
◖ the identity of parties to a transaction	☐	☐	☐
◖ parties to a transaction cannot later refute their participation.	☐	☐	☐
Agency websites contain statements establishing their intended purpose and legal use and the implications of inappropriate use.	☐	☐	☐
The legal rights over website names have been clearly established.	☐	☐	☐
Statements about legal liability and proper use are displayed prominently on agency websites.	☐	☐	☐
Third party partner agreements specify:			
◖ the liability exposure and remedy options of each party	☐	☐	☐
◖ data ownership and rights.	☐	☐	☐

Customer Readiness and Accessibility

E-GOVERNMENT SERVICES ARE DESIGNED HAVING REGARD TO CUSTOMER READINESS WHILE RECOGNISING THE BENEFITS OF ON-LINE SERVICE DELIVERY

BETTER PRACTICE PRINCIPLES

- The readiness of customers, their demand for electronic services, and what will benefit them most are carefully researched and assessed
- Electronic services are available to all parties expected to be served
- Customers know the services available electronically and the benefits of using them
- Traditional service delivery channels are retained, where necessary, to ensure equity or because the service can not be provided electronically
- Electronic services are accessible to those with special requirements such as disability, language, or literacy
- Fees charged are evaluated for user acceptance and fairness
- Electronic services are easy to use and help is available to users
- Customers are actively encouraged to utilise the Internet and related technologies

RISKS TO BE MANAGED

- People with restricted access to electronic services not well served
- New delivery methods not used sufficiently
- Customer demands exceed available capability or capacity
- Failure to include accessibility in system design increases project costs over the long run
- Legal action for discrimination
- Less efficient and effective delivery methods retained for longer than necessary

HELP

- ANAO, Internet delivery decisions - A Government Program Manager's Guide, components 1, 3, 5 and 9
- National Electronic Commerce Coordinating Council (US): E-government strategic planning - A White Paper; Risk assessment guidebook for e-government/e-commerce; Critical business issues in the transformation to electronic government
- NSW Office of Information Technology: memoranda, guidelines, case studies (various)

Checklist

	Performing	Progressing	Potential
Customer research is undertaken to establish:			
◖ expected use of electronic services	☐	☐	☐
◖ preferred approaches to electronic service delivery, including preferred medium (eg computer, telephone)	☐	☐	☐
◖ that electronic services are generally available to targeted users	☐	☐	☐
◖ satisfaction with electronic services.	☐	☐	☐
Electronic service delivery reflects customer research.	☐	☐	☐
Electronic service delivery is designed around what the customer wants to do, rather than around the structure of the agency.	☐	☐	☐
Traditional service delivery channels are retained where required so that customers are not disadvantaged.	☐	☐	☐
Strategies to raise customer use of the Internet and related technologies are implemented.	☐	☐	☐
Accessibility for individuals with special requirements is part of the standards for design of electronic services.	☐	☐	☐
Where appropriate, electronic services are available outside normal business hours for the convenience of users.	☐	☐	☐
The Government's access and pricing policy is followed.	☐	☐	☐
Any user fees required in addition to the traditional charge:			
◖ do not prevent the bulk of customers from using the electronic option	☐	☐	☐
◖ are not excessive compared to the traditional charge.	☐	☐	☐
There is no requirement upon users for special hardware or software to access the website.	☐	☐	☐
Methods are employed to make the electronic service option easy to use (such as touch screens and on-line help).	☐	☐	☐
Methods, tools or training are provided to assist individuals who lack the skills or have special requirements for accessing electronic services.	☐	☐	☐
Assistance, such as a help desk, is provided during hours that meet customer needs.	☐	☐	☐

Privacy

PRIVACY NEEDS TO BE PROTECTED TO ENSURE CONFIDENCE IN E-GOVERNMENT, WHILE ALLOWING FAIR AND REASONABLE INFORMATION SHARING TO SECURE POTENTIAL BENEFITS FOR CUSTOMERS AND GOVERNMENT

BETTER PRACTICE PRINCIPLES

- A privacy policy for e-government, consistent with legislative requirements, is established and disclosed
- Use of personal information is transparent
- A method for classifying information and for protecting sensitive information is established to prevent its unauthorised disclosure or access
- The potential benefits of information sharing for service quality and efficiency are considered in the development of privacy policies and classification systems
- Record retention and disposal policies are established and consistent with statutory requirements
- The use of information is monitored regularly to ensure compliance with policies and law
- There are appropriate sanctions for breaches of privacy

RISKS TO BE MANAGED

- Inappropriate granting or refusal of access to information
- Public concerns over adequacy of privacy protection
- Failure to comply with legal requirements for privacy and records management
- Potential benefits of increased information sharing lost due to privacy concerns
- Public perception of failure to live up to privacy/confidentiality undertakings
- Litigation for breach of privacy

HELP

- ANAO, Internet delivery decisions - A Government Program Manager's Guide, component 8
- NSW Office of Information Technology; Privacy guidelines (in preparation)
- Privacy NSW, A guide to information protection principles
- Privacy NSW, Privacy and Personal Information Protection Act, a plain English guide
- National Electronic Commerce Coordinating Council (US): E-government strategic planning - A White Paper; Risk assessment guidebook for e-government/e-commerce; Critical business issues in the transformation to electronic government; Privacy policies - Are you prepared?
- International Standards Accreditation Board, International e-commerce standard for security, privacy and service (business to business, and business to consumer)

Checklist

	Performing	Progressing	Potential
An e-government privacy policy forms part of the privacy management plan, developed in line with statutory requirements and in consultation with Privacy NSW.	☐	☐	☐
The e-government privacy policy is regularly reviewed.	☐	☐	☐
An electronic record management policy has been developed in line with statutory requirements and in consultation with State Records.	☐	☐	☐
The privacy and electronic records management policies promote fair and reasonable information sharing where there are benefits to efficiency and effectiveness.	☐	☐	☐
Wherever and whenever individually identifiable information is requested, there is clear disclosure of:			
◖ the information collected and how it is collected	☐	☐	☐
◖ the intended use of information collected and how it will be disposed of	☐	☐	☐
◖ whether the information is shared with third parties, who they are, what information is shared, and the purpose for sharing	☐	☐	☐
◖ whether individuals may choose not to have their personal information collected or shared with third parties	☐	☐	☐
◖ how the agency maintains the accuracy and security of the individually identifiable information it receives and stores	☐	☐	☐
◖ how individuals may review their information and request corrections	☐	☐	☐
◖ any information that is collected or exchanged involuntarily (such as 'cookies')	☐	☐	☐
◖ how to contact the agency regarding the privacy policy.	☐	☐	☐
Practices are monitored to ensure adherence to privacy and records management policies.	☐	☐	☐
Information is classified and assigned a protection level according to relevant statutory disclosure restrictions or its sensitivity.	☐	☐	☐
Data classification is periodically reviewed to ensure that information collected and stored is classified and stored correctly, and is still required.	☐	☐	☐
Data custodianship is defined for any data that is disclosed to or received from third parties.	☐	☐	☐
Restrictions on disclosure are formally agreed to by personnel and third parties with access to confidential information.	☐	☐	☐
Appropriate sanctions are imposed for violating confidentiality restrictions.	☐	☐	☐

Security

AN EFFECTIVE SECURITY SYSTEM, DESIGNED TO PROTECT NETWORK, APPLICATIONS AND DATA, IS ESSENTIAL TO E-GOVERNMENT

BETTER PRACTICE PRINCIPLES

- A comprehensive approach to security is adopted, including policies, education, physical protection, security software and manual security procedures
- A risk management approach to determining levels of security is adopted
- Security measures are reviewed, monitored and tested regularly
- Security is considered at the design and implementation stages
- Interconnecting partners are required to adopt similar security standards
- All personnel are held accountable for ensuring system security

RISKS TO BE MANAGED

- Inadequate security awareness among personnel
- Lack of capability to address security issues
- Programs or information improperly introduced, modified or deleted
- Viruses and hacker attacks disrupt or embarrass the agency
- Inability to operate in the event of a major system disruption
- Security concerns prevent partnering with other organisations

HELP

- ANAO, Internet delivery decisions - A Government Program Manager's Guide, component 6
- Information Systems Audit and Control Foundation, e-Commerce security: enterprise best practices
- NSW Office of Information Technology: memoranda; guidelines; case studies (various)
- NSW Treasury, Risk Management and Internal Control Toolkit
- National Electronic Commerce Coordinating Council (US): E-government strategic planning - A White Paper; Risk assessment guidebook for e-government/e-commerce; Critical business issues in the transformation to electronic government
- PricewaterhouseCoopers, E-business risks: Can your organisation be trusted?
- Office for Government On-line (Cwth), On-line action plan guidelines
- International Standards Accreditation Board, International e-commerce standard for security, privacy and service (business to business and business to consumer)
- ICAC, The Need to Know: eCorruption and Unmanaged Risk

Checklist

	Performing	Progressing	Potential
Security is a key consideration in e-government planning, development and operation.	☐	☐	☐
Security policies, plans and procedures:			
◖ conform with the Information Security Guidelines which are based on the relevant Australian Standard	☐	☐	☐
◖ are documented and communicated to personnel and third parties that have access to systems, data or facilities.	☐	☐	☐
An information systems security manager has been nominated and is carrying out activities in accordance with government guidelines.	☐	☐	☐
Risk assessments are regularly performed to respond to changes to the system or operating environment.	☐	☐	☐
Security is a shared responsibility within the agency, and personnel are held accountable for it.	☐	☐	☐
Ongoing security training is conducted for all relevant personnel.	☐	☐	☐
Connecting partners are certified to the Australian Standard.	☐	☐	☐
Effective mechanisms are in place to:			
◖ offer protection from threats, including viruses, hackers and saboteurs	☐	☐	☐
◖ allow secure communication across the Internet, protecting the traffic from inappropriate disclosure or modification	☐	☐	☐
◖ uniquely and positively identify participants to an electronic transaction	☐	☐	☐
◖ ensure that participation in a transaction cannot be refuted later.	☐	☐	☐
E-government systems are comprehensively and regularly tested and reviewed to provide assurance that controls are present and effective.	☐	☐	☐
Ongoing testing and review includes:			
◖ Penetration test: A 'real life' test of the security of the Internet or dial in remote access connections from the outside	☐	☐	☐
◖ Diagnostic review: A detailed internal review of those parts of the system relevant to security	☐	☐	☐
◖ General Controls Review: Review of general controls, including policies and procedures.	☐	☐	☐
There is a system in place to recognise security breaches.	☐	☐	☐
Unauthorised activity and system vulnerabilities are addressed.	☐	☐	☐
Individual access to systems and information is properly controlled.	☐	☐	☐
The agency's disaster recovery planning deals with e-government issues, and is reviewed regularly.	☐	☐	☐

Technology and Information Management

SYSTEMS SHOULD BE DEVELOPED WITH THE FLEXIBILITY TO ACCOMMODATE CHANGES IN TECHNOLOGY AND PROVIDE A CONTINUED ABILITY TO SHARE INFORMATION

BETTER PRACTICE PRINCIPLES

- Systems are flexible and can be upgraded and expanded to allow them to evolve with e-government developments
- Systems readily integrate and share information within the agency and with third parties
- A formal and robust process is used to select or develop technical solutions
- Standard products and solutions are used where feasible
- Consultation with related agencies and organisations promotes the introduction of compatible systems and information
- Care is taken to avoid becoming 'locked in' to particular solutions or suppliers
- Data is accurate, current, complete and processed appropriately
- Data is in a form which can be readily shared with other relevant organisations (to the extent allowable)

RISKS TO BE MANAGED

- Technologies not designed or implemented properly
- Unproven technologies used causing system failure
- Technologies not adequate for current and projected requirements resulting in poor performance, availability and reliability
- Systems not interacting effectively resulting in inefficient processes
- Information held in existing systems not accessed or too much is spent on accessing such information
- Opportunities for enhanced sharing of information and technology between agencies not taken

HELP

- ANAO, Internet delivery decisions - A Government Program Manager's Guide, components 1, 2, 3 and 5
- NSW Office of Information Technology: memoranda; guidelines; case studies (various)
- connect.nsw, an Internet strategy for NSW and connect.nsw implementation framework
- National Electronic Commerce Coordinating Council (US): E-government strategic planning - A White Paper; Risk assessment guidebook for e-government/e-commerce; Critical business issues in the transformation to electronic government
- Office for Government On-line (Cwth), On-line action plan guidelines
- NSW Department of Public Works and Services, NSW Government eProcurement Implementation Strategy

Checklist

	Performing	Progressing	Potential
A formal system/application development methodology, designed for e-government, is used for all information and communications technology (ICT) projects.	☐	☐	☐
Government-wide procedures for the procurement of technology resources are followed.	☐	☐	☐
Government-wide standards and guidelines for exchanging and using information in a straightforward way (interoperability) are adopted.	☐	☐	☐
Standard applications are used wherever possible.	☐	☐	☐
System components are selected to ensure the agency does not become 'locked in' to a particular technology or supplier (ie open systems are adopted).	☐	☐	☐
Systems are designed to:			
◖ integrate with important internal and external databases and applications	☐	☐	☐
◖ change as needs change.	☐	☐	☐
Sector wide benefits are considered in determining whether and how information in existing systems should be accessed.	☐	☐	☐
There is ongoing communication with other relevant agencies to:			
◖ identify and explore opportunities for sharing technology resources	☐	☐	☐
◖ develop compatibility across IT systems	☐	☐	☐
◖ define and put data into a form which can be readily shared.	☐	☐	☐
Database management and monitoring techniques are employed to ensure that data is consistent, accurate, current, complete and processed appropriately.	☐	☐	☐
System performance and reliability standards are:			
◖ defined	☐	☐	☐
◖ monitored to ensure compliance.	☐	☐	☐
System changes are properly authorised and tested sufficiently.	☐	☐	☐
Ongoing monitoring is performed to ensure that unauthorised system changes have not occurred.	☐	☐	☐

The following is a list of some resources which may be useful. The web site addresses may be used to obtain these directly, or to request them via e-mail. These web sites may also provide other useful information not listed here.

Australian National Audit Office (www.anao.gov.au)
Internet delivery decisions: A government program manager's guide - best practice (2001)

Commonwealth Office for Government On-line (www.ogo.gov.au)
GovernmentOnline: On-line action plan guidelines (2000)

Independent Commission Against Corruption (www.icac.nsw.gov.au)
The need to know: eCorruption and unmanaged risk (2001)

Information Systems Audit & Control Foundation (www.isaca.org)
e-Commerce security - Enterprise best practices (2000)
Control Objectives for Information and related Technology (2001)

International Standards Accreditation Board (www.etick.com/index.html)

The international e-commerce standard for security, privacy & service (business to business) (2000)

The international e-commerce standard for security, privacy & service (business to consumer) (2000)

NSW Electronic Transactions Act 2000 (www.nsw.gov.au)

NSW Office of Information Technology (www.oit.nsw.gov.au)
Information management & technology blueprint for NSW: A well-connected future (1997)
connect.nsw: An Internet strategy for NSW (1997)
connect.NSW: Implementation framework (1998)
Memoranda
Guidelines
Case studies

NSW Premier's Department (www.premiers.nsw.gov.au)
Personnel handbook (2000)
Business case guidelines (2000)
Circulars
Memoranda

NSW Department of Public Works & Services (www.dpws.nsw.gov.au)
Risk management in electronic procurement: Strategies for implementation (2000)
Meeting the challenge: Electronic procurement implementation strategy (2001)

NSW Treasury (www.treasury.nsw.gov.au)
NSW Treasurer's Directions
Risk management and internal control toolkit (1996)
Circulars

PricewaterhouseCoopers (www.pwcglobal.com.au or www.iia.asn.au/issues.asp)
E-business risks: Can your organisation be trusted? Presentation by Mike O'Hehir to the NSW Audit Executives Network (2000)

Privacy NSW (www.lawlink.nsw.gov.au/pc.nsf)
Privacy & Personal Information Protection Act: A plain English guide (1999)
A guide to the Information Protection Principles (2000)

USA National Electronic Commerce Coordinating Council (www.ec3.org)
Critical business issues in the transformation to electronic government (2000)
Risk assessment guidebook for e-commerce / e-government (2000)
E-government strategic planning: A white paper (2000)